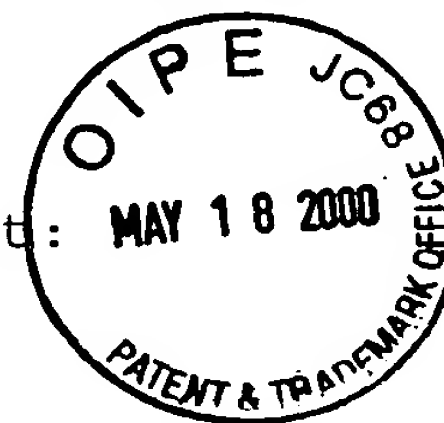


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: RUEDIGER BARTZ

Serial No.: 09/484,418

Group Art Unit:



Filed: JANUARY 18, 2000

Examiner:

Title: METHOD FOR AUTHENTICATING A SPARE KEY FOR USING A
VEHICLE

CLAIM FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of prior foreign application No. 199 01 277.6, filed in Germany on January 15, 1999, is hereby requested and the right of priority under 35 U.S.C. §119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of the original foreign application.

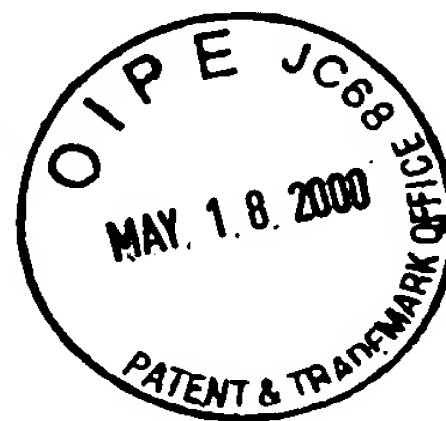
Respectfully submitted,

May 18, 2000

for Barry R Edwards 31824
Jeffrey D. Sanok
Registration No. 32,169

EVENSON, McKEOWN, EDWARDS
& LENAHA, P.L.L.C.
1200 G Street, N.W., Suite 700
Washington, DC 20005
Telephone No.: (202) 628-8800
Facsimile No.: (202) 628-8844

BUNDESREPUBLIK DEUTSCHLAND



Bescheinigung

Die Bayerische Motoren Werke Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

„Verfahren zum Authentisieren eines Ersatzschlüssels zum
Benutzen eines Fahrzeugs“

am 15. Januar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole B 60 R, G 07 C und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 22. Dezember 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Zitzenzier

Aktenzeichen: 199 01 277.6

Verfahren zum Authentisieren eines Ersatzschlüssels zum Benutzen eines Fahrzeugs

5

Die Erfindung bezieht sich auf ein Verfahren mit den Merkmalen des Oberbegriffs von Patentanspruch 1.

10

Ein derartiges Verfahren ist aus der EP 0 788 946 A bekannt. Dabei werden mit Hilfe eines separaten, außerhalb des Fahrzeugs befindlichen Programmiergeräts von einer Zentrale fahrzeugteilespezifische Daten abgefragt, die von der Zentrale an das Programmiergerät und von diesem an das Fahrzeug weitergegeben werden, um
15 dort decodiert zu werden. Obwohl dabei teilweise sogar mit einer doppelten Codierung gearbeitet wird, können beim bekannten Verfahren Probleme entstehen, wenn das Programmiergerät mißbräuchlich verwendet wird.

20

Insgesamt ist festzustellen, daß der allgemeine Trend die Diebstahl- und Einbruchssicherheit zu erhöhen, gegensinnig zu der Notwendigkeit des Kundendienstes verläuft, das Fahrzeug zu öffnen bzw. auch zu bewegen, wenn der Original- Schlüssel nicht vorhanden ist, was z.B. bei Verlust oder gar bei einem unabsichtlich im Fahrzeug eingesperrten Original- Schlüssel der Fall sein kann. Das Problem steigert sich noch beim Einsatz von einbruchshemmender Verglasung.

25

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art zu schaffen, das einfach im Ablauf und der Handhabung ist und das gegenüber einem Mißbrauch geschützt ist.

30

Die Erfindung löst diese Aufgabe mit den im Patentanspruch 1 angegebenen Mitteln.

Wesentlich für die Erfindung ist die Authentisierung des Ersatzschlüssels durch die Zentrale. Da die Identifikationsnummer des Ersatzschlüssels der Zentrale übermittelt und dort überprüft wird, kann die offensichtlich mißbräuchliche Verwendung eines beispielsweise verlorenen Ersatzschlüssels, sofern sie der Zentrale bekannt ist, erkannt und die Ausgabe des Freigabesignals von der Zentrale an das Fahrzeug verhindert werden.

Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der weiteren Patentansprüche und werden anhand des in den Figuren dargestellten Verfahrensablaufs näher erläutert.

Die einzige Figur zeigt ein Blockschaltbild, in dem die im Rahmen des erfindungsgemäßen Verfahrens wirksamen Schaltstellen und Übertragungswege gezeigt sind,

Das hier beschriebene Verfahren bietet die Möglichkeit zum Öffnen und zur Inbetriebnahme eines Fahrzeugs mit Hilfe eines universell verwendbaren Ersatzschlüssels ohne die Wirkung des Diebstahlschutzes zu verringern. Dabei wird mittels einer Authentisierung des Ersatz-Schlüssels durch eine Zentrale unter Nutzung des Autotelefons und einer zentralen Datenbank eine Berechtigung, mit Hilfe des Ersatzschlüssels das Fahrzeug zumindest zu öffnen, temporär erteilt.

Der universell verwendbare Ersatz-Schlüssel wird im folgenden VK-Key genannt. Weitere Wirkstellen im Rahmen des Verfahrens sind eine die zentrale Datenbank (genannt VK-Datenbank) ein im Fahrzeug vorhandenes Autotelefon, ein Basis-Interface Telefon (genannt BIT-Interface) sowie ein Mobiltelefon eines Kundendienstmitarbeiters, der den Ersatz-Schlüssel zur Anwendung bringt. Wesentlich ist ferner, daß für Telefonverbindungen vorzugsweise asynchrone Algorithmen verwendet werden. Dadurch besteht für die Telefonverbindungen keine Notwendigkeit, eine Abhörsicherheit zu erzielen. Unter einem asynchronen Algorithmus ist ein Verschlüsselungsverfahren zu verstehen, bei dem in einer Richtung mit einem öffentlichen Verschlüsselungsalgorithmus (public-key) und zur Entschlüsselung mit einem geheimen Verschlüsselungsalgorithmus (secret-key) gearbeitet wird.

Die Auswertung der im Fahrzeug eingehenden Signale wird bevorzugt durch das als Wegfahrsicherheitseinrichtung dienende CAS-Steuergerät (CAS= Car Access System) vorgenommen, das über einen Ringspeicher verfügt, in dem die erfolgreichen
 5 VK-Key Authentisierungen gespeichert und in einem Attack-Speicher evtl. Manipulationsversuche abgelegt sind.

Der gesamte Vorgang zum Öffnen des Fahrzeugs mit Hilfe des Ersatz-Schlüssels vollzieht sich in 5 Stufen I-V .

10

I) Durch Betätigen einer Befehlstaste am VK-Key generiert der Ersatz-Schlüssel eine Zufalls-Zahl PIN, die einerseits unverschlüsselt und andererseits zusammen mit einer individuellen Kennung des Ersatz-Schlüssels VK_KEY_ID mit einem nicht geheimen (=öffentlichen) Code verschlüsselt an das Fahrzeug übertragen wird. Das Fahrzeug nimmt über einen Funkempfänger dieses drahtlos übertragenene, verschlüsselte Signal $Krypt_{fl}(VK_KEY_ID, PIN)$ und die Zufalls-Zahl PIN auf und leitet sie dem CAS zu, wo die Kennung des Ersatz-Schlüssels VK_KEY_ID aufgrund der Kenntnis der Zufalls-Zahl PIN entschlüsselt wird.

15

20 II) Der Servicetechniker überträgt vorzugsweise mittels seines Mobiltelefons an die VK-Datenbank folgende Daten:
 Zufalls-Zahl PIN, sowie die Telefonnummer und Fahrgestellnummer des Fahrzeugs. Bei einer telefonischen Übermittlung ist eine Codierung nicht erforderlich.

25

Die VK-Datenbank holt unter Verwendung der Fahrgestellnummer den entsprechenden Public-Key des Fahrzeugs (P-CODE - FZG) und verschlüsselt die Zufalls-Zahl PIN damit.

30 III) Von der VK-Datenbank aus wird das Telefon des Fahrzeugs angewählt und die so verschlüsselte Zufalls-Zahl PIN übertragen, welche dort empfangen und an das CAS-Steuergerät weitergeleitet wird. Das CAS besitzt einen geheimen Ent-

schlüsselungsalgorithmus Secret- Key (S-CODE-Fzg), der es in die Lage versetzt, ohne eigentliche Kenntnis der Zufalls-Zahl PIN diese PIN rückzubilden. Die PIN wird dann mit der im Schritt I erhaltenen verglichen.

- 5 IV) Sind die beiden PINs identisch, erzeugt das CAS eine eigene Zufallszahl RAND. RAND und die dorthin im Schritt I übertragenen Kennung VK_KEY-ID des Ersatz-Schlüssels werden jedes für sich mit einem Public Key P-CODE-VK verschlüsselt und über das Telefon des Fahrzeugs an die VK-Datenbank übertragen.
- 10 Dort wird mittels des Secret Key S-CODE-VK der VK-Datenbank die Zufallszahl RAND und der VK-Key-Identifizier VK_KEY-ID rückgebildet und überprüft, ob der VK-Key-Identifizier VK_KEY-ID einem gültigen Ersatz-Schlüssel zugeordnet ist. Für diese Rückbildung ist die separate Kenntnis der Zufallszahl RAND nicht erforderlich.
- 15 V) Ist der VK-Key-Identifizier gültig, so wird als Rückmeldung die Zufallszahl RAND mit einem Public-Key P - CODE-Fzg verschlüsselt und an das CAS ins Fahrzeug übertragen. Dieses kann mit seinem Secret Key S-CODE-Fzg die Zufallszahl RAND rückbilden und mit der in seinem Speicher vergleichen. Sind die
- 20 beiden identisch, so wird dies als Bestätigung der Gültigkeit des Ersatz-Schlüssels VK_Key ausgelegt und mit dem VK_Key aufgegebene Befehle ausgeführt.

Patentansprüche

5

1. Verfahren zum Authentisieren eines Ersatzschlüssels zum Benutzen eines
Fahrzeugs ohne den regulären Schlüssel,
dadurch gekennzeichnet, daß der Ersatzschlüssel eine
10 Identifikationsnummer besitzt, die einer Zentrale übermittelt und dort
überprüft wird und daß der Ersatzschlüssel durch Aufgabe eines
Freigabesignals von der Zentrale an das Fahrzeug authentisiert wird.
2. Verfahren nach Anspruch 1,
15 dadurch gekennzeichnet, daß die Datenübermittlung vom Ersatzschlüssel
zur Zentrale und/oder von der Zentrale zum Fahrzeug und/oder vom
Ersatzschlüssel zum Fahrzeug codiert vorgenommen wird.
3. Verfahren nach Anspruch 2,
20 dadurch gekennzeichnet, daß die Datenübermittlung in einer Richtung von
der Übermittlung eines Bestätigungssignals in entgegengesetzter Richtung
gefolgt wird.
4. Verfahren nach Anspruch 3,
25 dadurch gekennzeichnet, daß der bidirektionale Datenverkehr in der einen
Richtung auf der Basis eines Public-Keys und die Entschlüsselung in der
Gegenstation auf der Basis eines Private-Keys erfolgt.

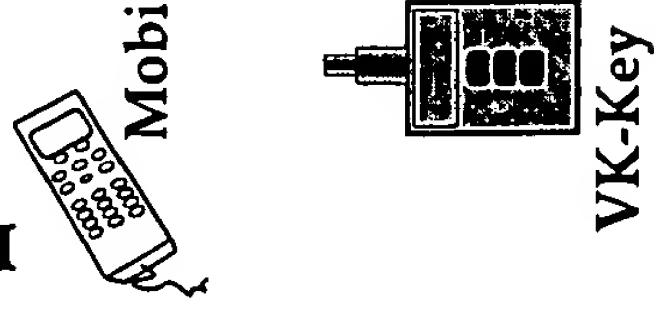
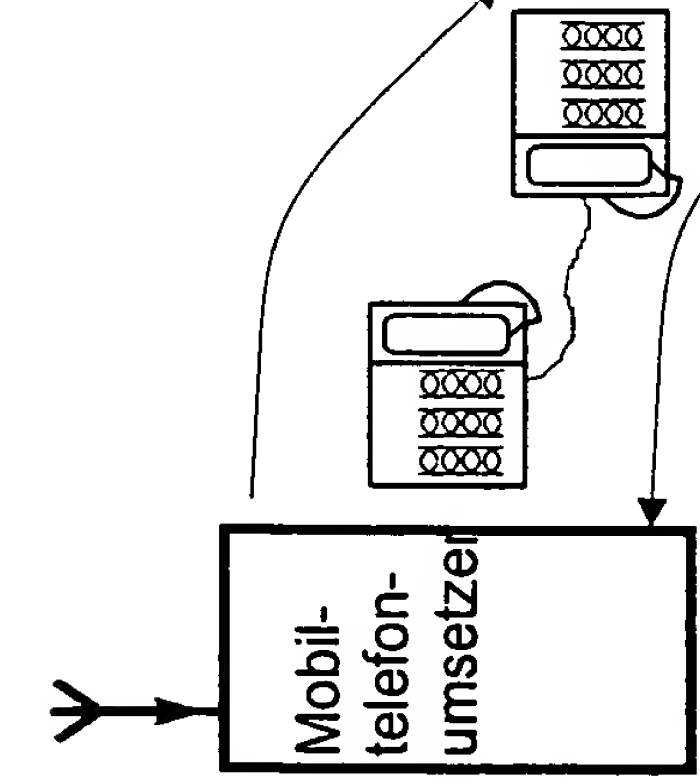
5. Verfahren nach den Ansprüchen 1 bis 4,
dadurch gekennzeichnet, daß die Übermittlung der Identifikationsnummer
des Ersatzschlüssels an die Zentrale durch das Fahrzeug selbst
5 vorgenommen wird, an das die Identifikationsnummer vorbereitend vom
Ersatzschlüssel übertragen wird.
6. Verfahren nach den Ansprüchen 1 bis 5,
dadurch gekennzeichnet, daß die Datenübermittlung per Telefon
10 vorgenommen wird.
7. Verfahren nach den Ansprüchen 1 bis 6,
dadurch gekennzeichnet, daß die Datenübermittlung mit einer Zufallszahl
codiert vorgenommen wird.
15
8. Verfahren nach den Ansprüchen 1 bis 7,
dadurch gekennzeichnet, daß vor der eigentlichen Datenübermittlung der
Empfänger durch den Ersatzschlüssel aktiviert wird.
20

Zusammenfassung

5

10

Bei einem Verfahren zum Authentisieren eines Ersatzschlüssels zum Benutzen eines Fahrzeugs ohne den regulären Schlüssel, besitzt der Ersatzschlüssel eine Identifikationsnummer, die einer Zentrale übermittelt und dort überprüft wird. Der Ersatzschlüssel wird durch Aufgabe eines Freigabesignals von der Zentrale an das Fahrzeug authentisiert.



II. Fahrgestellnummer + Telefonnummer Fzg. + PIN

IV.

V.

IV. $\text{Krypt_f3}(\text{VK_KEY_ID}, P\text{-Code_VK}) + \text{Krypt_f3}(\text{RAND}, P\text{-Code_VK})$

V. Krypt_f2(RAND,P-Code-FZG)

I. Krypt_f1(VK_KEY_ID,PIN)+PIN

VK-Key